REMARKS

Claims 1-11 have been examined, with all claims rejected.

Claims 1-11 have been provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-14 of copending application no. 10/827,913. In response, Applicant submits herewith a terminal disclaimer. Withdrawal of this rejection is therefore respectfully requested.

Claims 1-11 have been rejected under 35 USC 103(a) as being unpatentable over Shamir (U.S. Patent No. 5,991,415) in view of Boneh et al. (U.S. Patent No. 6,965,673; hereinafter "Boneh"). Applicant respectfully traverse this rejection for the reasons set forth below.

The Examiner states on page 4, penultimate paragraph, of the Office Action that Shamir discloses any verification "following" the combining step. This is, however, not correct. The combining step corresponds to step 30 of Fig. 2 of Shamir, in which the final result is computed by the Chinese Remainder Theorem. In particular, one might say that y_1, and y_2 calculated in box 28 correspond to the first auxiliary quantity and the second auxiliary quantity. See column 6, lines 37-38. Therefore, Shamir is completely silent an verifying the result of the exponentiation calculation, i.e., the result of the combing step (the result of the combining step is the "result" of the exponentiation calculation). Shamir instead teaches using s y_1, y_2 (which are definitely not the result of the combining step), in order to finally check whether the whole calculation was in order or not. Thus, when block 36 determines that the quality is not there, then an "abort is commanded for a faulty computation," as stated in column 6, lines 48-49, of Shamir. Therefore, the Examiner is not correct when stating that Shamir discloses any verifying step which is conducted <u>following</u> the combining step.

Boneh discloses certain types of faults which may occur permitting certain crypto systems to be cracked. See column 5, lines 50-54. Specifically, the RSA-CRT systems are mentioned as being specifically vulnerable to hardware fault attacks with only a single faulty signature. See column 9, lines 41-43. As a general rule, it is outlined that the output of a computation is to be checked before

releasing it. However, this is only a general statement in column 17, lines 16-17, without providing specific details. Then, in column 17, line 42, it is specifically stated that the use of blinding is useful for RSA computations which do not use the Chinese Remainder Theorem. Therefore, Boneh is completely silent on how to avoid any fault attacks on systems using RSA computations based on the Chinese Remainder Theorem.

This, however, is the field to which the present application is directed, as outlined in the preambles of independent claims 1 and 11.

Furthermore, it is a specific feature of the Chinese Remainder Theorem that two auxiliary quantities are calculated which are then combined to obtain a result of the exponentiation calculation. Importantly, the combining step as defined in claim 1 cannot be any combining step. Instead, this combining step has to be such that at the output of the combining step, the result of the exponentiation calculation is there. This is a typical characteristic of the Chinese Remainder Theorem, which subsequent for the combining step, outputs the result of the exponentiation calculation. In view of this, Boneh does also not suggest verifying the result of the exponentiation calculation following the combining step.

Similarly, the combiner in claim 11 can not be any combiner.

Therefore, even a combination of documents Shamir and Boneh would not result in the inventive method and device as defined in the claims.

In view of the above, Applicant believes the pending application is in condition for allowance.

In the event a fee is required or if any additional fee during the prosecution of this application is not paid, the Patent Office is authorized to charge the underpayment to Deposit Account No. 50-2215.

Dated: December 11, 2007

Respectfully submitted,

By Laura C. Brutman

Laura C. Brutman
Registration No.: 38,395
DICKSTEIN SHAPIRO LLP
1177 Avenue of the Americas
New York, New York 10036-2714
(212) 277-6500
Attorney for Applicant